サイバーセキュリティ情報遠隔分析基盤 NONSTOP の利活用について

竹久 達也 †‡　神薗 雅紀 †*　笠間 貴弘 †　中里 純二 †　衛藤 将史 †
井上 大介 †　中尾 康二 †

† 情報通信研究機構
184-8795 東京都小金井市貫井北町 4-2-1
{t.takehisa, masaki_kamizono, kasama, nakazato, eto, dai, ko-nakao}@nict.go.jp

‡ 株式会社ニッシン
665-0047 兵庫県宝塚市亀井町 10-7

* 株式会社セキュアブレイン
102-0083 東京都千代田区麹町 2-6-7 麹町 RK ビル 4F

あらまし サイバーセキュリティ分野の研究開発では，攻撃トラフィックやマルウェア検体等の“ 実データ ”を研究対象として実験利用することが必須である．情報通信研究機構が研究開発中のインシデント分析センタ NICTER は，これら実データを大量に収集・保有しており，NICTER が保有しているサイバーセキュリティ情報を遠隔から安全に利用するための分析基盤 NONSTOP を，本分野における研究機関に対して提供している．また，MWS2013 以降データセット提供プラットフォームとしての利活用も進んでいる．本稿では，データセット提供プラットフォームとしての NONSTOP の改良点，追加機能を示し評価を与える．

Utilization of Secure Remote Analysis Platform for Cybersecurity Information(NONSTOP)

Tatsuya TAKEHISA†‡　Masaki KAMIZONO†*　Takahiro KASAMA†
Junji NAKAZATO†　Masashi ETO†　Daisuke INOUE†　Koji NAKAO†

†National Institute of Information and Communications Technology.
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, JAPAN
{t.takehisa, masaki_kamizono, kasama, nakazato, eto, dai, ko-nakao}@nict.go.jp

‡Software Section, Technical Department, Nissin inc.
10-7 Kamei-cho, Takarazuka, Hyogo 665-0047, JAPAN

* Securebrain Corporation
Kojimachi RK Bldg, 2-6-7 Kojimachi, Chiyoda-ku, Tokyo 102-0083, JAPAN

Abstract In the field of Cyber-Security Research, it is greatly essential for researchers to utilize a set of live attack traffic and malwares executable samples and so on. NICT has been working for Incident Analysis Center called NICTER which has been collecting a huge volume of real traffic data (such as scan data) and has developed NONSTOP system for the purpose of providing real traffic data for their research activities based on the remote access in secure manner. Provision of data set has been carried out since MWS2013 based on the platform of NONSTOP. In this paper, functions required for the improvement of NONSTOP system and their evaluation will be provided.

1　はじめに

刻一刻と進化するサイバー攻撃に対抗するために，サイバーセキュリティ分野の研究開発は重要性を増している．本分野で研究開発を行うには，サイバーセキュリティ情報（攻撃トラフィックやマルウェア検体など）を取得し，実験利用することが必須である．しかし，これら実データを定常的に収集し，維持管理するのは，それ相応のコストと技術力が必要となり，本分野へ対して研究開発・参入する障壁となっている．

そのため，近年においては国内外においてサイバーセキュリティ情報の公開・共有が盛んであり，国内では，コンピュータセキュリティシンポジウムと合同開催されているマルウェア対策研究人材ワークショップ (MWS) において，サイバーセキュリティ情報を共有し，研究に利活用できる環境作りを行っている．

上記の様な，サイバーセキュリティ情報の公開･共有の取り組みを行ってはいるが，サイバーセキュリティ情報には，取り扱いに注意すべき機微な情報（マルウェア検体や個人情報，機密情報）が含まれている可能性も有り，公開・共有する際には，限定的な情報とならざるを得ない．このことは，サイバーセキュリティ情報を利用する研究者に対しての制約となっている．

情報通信研究機構（NICT) では，ネットワークインシデントの早期検出と迅速な原因究明を実現するためにインシデント分析センター NICTER[1][2][3] [1]の研究・開発を進めている．NICTER では，日本国内外に点在する複数のダークネットにブラックホールセンサを設置し，定常的な観測を行っている．また，マルウェア検体の収集・動的な解析も実施し，ダークネットからのパケットとマルウェア検体との相関分析も行っている．さらに，収集･分析されたデータは，視覚情報として可視化され，オペレータによる常時監視し，サイバー攻撃インシデント発生時においては，関係各所へ情報提供を行っている．一部の情報は，サイバー攻撃情報を公開するためインターネット上にて一般公開している [4].

そこで，NICT では，収集したサイバーセキュリティ情報（以下，NICTER リソース）の外部研究者による利活用を推進するために，NICTER が保有しているサイバーセキュリティ情報を遠隔から安全に利用するための分析基盤 NONSTOP[5] [2]を研究･開発している．NONSTOP の開発以前は，NICTER リソースを遠隔利用することができず，外部研究者の制約となっていたが，NONSTOP の実験運用開始以後は，外部研究者が遠隔から NICTER の保有するサイバーセキュリティ情報を分析できるようになった．さらに，2013 年の MWS からは，MWS から提供される研究用データセットの一つであるダークネットトラフィック（NICTER Darknet Dataset）の提供を行う基盤として利活用され，サイバー攻撃に関する研究者の人材育成，研究の発展に対して大きく貢献している．また，MWS2014 では，規定時間内に研究用データセットについての課題に取り組む MWS Cup において，事前課題の一つであるダークネットトラフィックの提供基盤として NONSTOP が利用される．

本稿では，NONSTOP システム（以下，本システム）の全機能を有するバージョン（以下，FULLSET 版）から，MWS におけるデータセット提供基盤（以下，MWS 版）としての修正点，変更点を述べる．

以下，2 章では，本システムの概要を述べ，3 章では，修正・変更点を示し，4 章では，可用性を評価し，5 章にてまとめる．

2　NONSTOP システム概説

図 1 は，本システムの概要図である．

本章では，本システムが有する機能について概略を述べる．

NONSTOP は，主に以下の機能を有する．

1) リモートログイン機能

2) 分析環境提供機能

3) NICTER リソース提供機能

[1]Network Incident analysis Center for Tactical Emergency Response の略

[2]Nicter Open Network Security Test-Out Platform の略

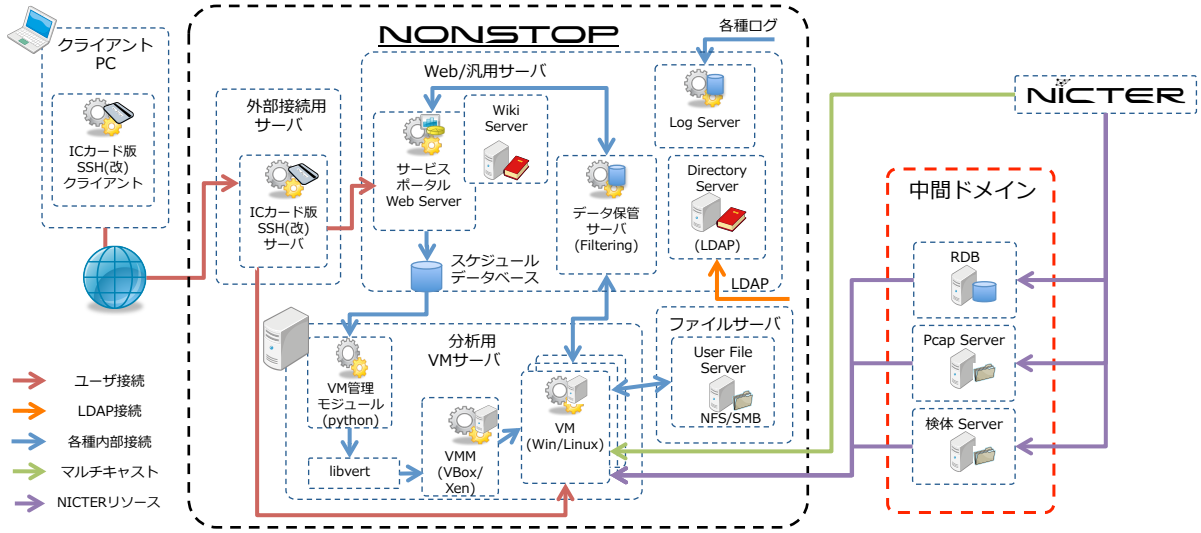

図 1: NONSTOP システム概要図

4) ファイル転送機能

5) ユーザ支援機能

以下では，各機能の簡単な説明を行う．

2.1 リモートログイン機能

ユーザは，まず，本システムを利用ため，NICT から提供される IC カードを入手する必要がある．そのために，ユーザは，NICT へ NONSTOP の利用申請をおこなう．NICT では，利用申請時に記載された情報（利用者情報，利用者接続元 IP アドレスなど）から，IC カードを発行し，ユーザへ送付する．

ユーザは，本システムへリモートログインするために，入手した IC カードを使って，IC カード認証可能な SSH クライアントにてログインする．

本機能では，リモートログイン機能を実現するための実装として，OpenSSH を改造したものを利用している．OpenSSH の改造点として，特定ポート以外へのポートフォワード禁止，ターミナルログインの禁止，通信帯域制限を行っている．また，外部と接続している Firewall に対しては，登録されている利用者接続元 IP 以外からの受信は禁止するようにしている．

2.2 分析環境提供機能

本システムでは，ユーザに対しインシデント分析を行う環境として，仮想マシン (VM;Virtual Machine) を提供する．これは，クラウドコンピューティングにおける PaaS(Platform As A Service) の形態であり，ユーザは，与えられた VM で自由に解析プログラムを実行することが可能である．

ユーザは，どの様な研究を行うかによって，仮想マシン環境として以下の解析環境のいずれかが提供される．

1) マクロ解析環境
マクロ解析環境は，主にダークネットトラフィック (リアルタイム，静的) を用いる場合に提供される．マクロ解析環境の VM で動作させる OS として，Windows XP, 7, Linux(CentOS) のいずれかが提供される．

2) 静的ミクロ解析
静的ミクロ解析環境は，マルウェア検体を解析環境にて実行せず静的（バイナリ列として）に解析する場合，また，マルウェア動的解析結果（ミクロ解析結果）のみを利用する場合に提供される．静的ミクロ解析環境の VM で動作させる OS として，Linux が提供される．

3) 動的ミクロ解析

動的ミクロ解析環境は，マルウェア検体を解析環境にて実行させ解析する場合に提供される．動的ミクロ解析環境は，前述の 1,2) とは違い，VM は 2 台提供され，それぞれ，マルウェア分析側 VM(Debugger) と，マルウェア実行側 VM(Debuggee) である．動的ミクロ解析環境の VM で動作させる OS として，Windows XP, 7 のいずれかが提供される．

解析環境に対して，ユーザは，RDP(Remote Desktop Protocol）を通じてアクセスを行う．

2.3 NICTER リソース提供機能

NONSTOP で，ユーザに提供する NICTER リソースを以下に示す．

1) リアルタイムダークネットトラフィック
   NICTER のブラックホールセンサに届いたダークネットトラフィックをリアルタイムに解析する際に利用する．

2) 静的ダークネットトラフィック（PCAP ファイル）
   NICTER のブラックホールセンサに届いたダークネットトラフィックを 24 時間毎に PCAP 形式でファイル化したもので，過去にさかのぼって解析する際に利用する．

3) マルウェア検体
   NICTER で収集しているマルウェア検体であり，本システムの解析環境上で静的または動的に検体を解析する際に利用する．

4) マルウェア動的解析結果
   NICTER では収集したマルウェア検体を，NICTER システム内で稼働している動的解析システムにて自動的に解析を行っており，その動的解析結果を用いて解析する際に利用する．

2.3.1 中間ドメイン

本システムでは，NICTER と本システムの間に，中間ドメインと呼ぶ NICTER リソース提供用の境界を設けている．中間ドメインの役割は，NICTER の収集・保有している NICTER リソースに含まれる機微な情報をフィルタリングし，本システムに対して前述の NICTER リソースを提供する機能を担う．

中間ドメインに配置された，各サーバの機能を以下に示す．

- PCAP サーバ
  一日ごとに，NICTER からの PCAP ファイルを受け取る．受け取った PCAP ファイルは，ダークネットの着信 IP アドレスは匿名化された状態である．

- ミクロ解析結果サーバ
  一日ごとに，NICTER が動的解析した結果を受け取る．

- 検体サーバ
  一日ごとに，NICTER で収集した本システムに提供可能なマルウェア検体を受け取る．

- パケットフィルタ（匿名化）
  リアルタイムに，NICTER が観測したダークネットトラフィックを受け取る．受け取ったダークネットトラフィックの，着信 IP アドレスは匿名化し，本システムへ転送する．

- RDB(Relational Database)
  PCAP サーバの内容と同じ内容を受け取り RDB へ格納している．

ユーザは，各解析環境 (VM) から，中間ドメインに配置された各サーバ，フィルタ，RDB をアクセスすることにより，NICTER リソースを利用することが可能となっている．

2.4 ファイル転送機能

本システムでは，分析環境で分析した結果や，ユーザ独自のデータ，ソースコードなどを分析環境に転送する場合，ユーザは，本システム内に構築された Web サーバを通じ，WebDAV プロトコルを用いて分析環境である VM に対してファイルの転送を行うことが出来る．ファイル転送機能では，ユーザが VM に対してファイルを転送する場合は Import とし，ユーザが

VM からファイルを取得する場合は Export として表現する．本システムでは，VM からファイルを Export する場合には，NICTER リソース（PCAP ファイル，マルウェア検体など）など，外部に流出させてはいけないファイルの転送が行われていないかフィルタリングするために逐次チェックする．フィルタリングのルールとしては，

1) マルウェア検体などのファイル Hash 値によるチェック
2) ファイル種別によるチェック
3) 暗号化・圧縮されていないかのチェック
4) ファイルサイズのチェック

があり，フィルタリングするプログラム（ルール）は状況に応じて拡張可能となっている．そして，フィルタリングルールによって NG となったイベントログは，Export トレース DB へ格納され，VM から Export するために書き込んだファイルは削除し，どの様なファイルを転送しようとしたのかオペレータによってチェックされる．また，VM から Export されたファイルはすべて Export トレース DB へ格納する．この様な仕組みとなっているため，オペレータはユーザが本システムからどの様なファイルを取得したのかトレースが可能となっている．

2.5 ユーザ支援機能

本システムを利用するユーザを支援するため，本システム内にサービスポータルとして Web サーバによるインターフェースを提供している．この Web サーバでは，利用者が解析環境の利用期間申請や解析環境 VM の Power ON/OFF, Reset が可能である．また，Wiki サーバも構成しており，ユーザへの情報発信やトラブルシューティング情報を掲載することで，利便性を向上させている．さらに，動的ミクロ解析環境にて，NICTER リソース中のマルウェア検体を解析するため，Web インターフェース上で指定したマルウェア検体を，動的ミクロ解析環境の Debuggee 用 VM の Import フォルダに対してコピーする機能も有する．

3 NONSTOP for MWS

本章では，本システム FULLSET 版のサブセットである MWS 版への変更・修正点を述べる．

1) MWS 用 NICTER リソース提供機能

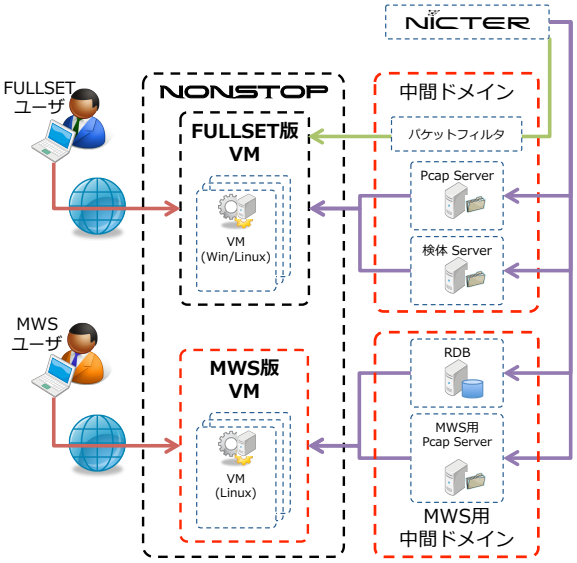

図 2: 中間ドメイン接続図

FULLSET 版で提供する NICTER リソースと MWS 版で提供する NICTER リソースでは，提供するデータセットの範囲が異なる．そのため，MWS 版として提供される NICTER リソースは，静的ダークネットトラフィック（PCAP ファイル）と，PCAP ファイルと同じ内容が格納された RDB のみであり，FULLSET 版で提供されているリアルタイムダークネットトラフィック，マルウェア検体，マルウェア動的解析結果は提供されない．

MWS 版として部分提供される NICTER リソースを提供する中間ドメインとして，新たに MWS 用中間ドメインを図 2 で示すように追加した．FULLSET 版 VM が接続される中間ドメインと，MWS 版 VM が接続される中間ドメイン（MWS 用中間ドメイン）は，物理的に接続を分けることで，アクセス可能なリソースへのアクセス制限を行っている．

2) MWS 版分析環境提供機能

MWS 版では，FULLSET 版で提供している，マクロ解析環境，静的ミクロ解析，動的ミクロ解析の内，マクロ解析環境のみを提供している．これは，1) で述べたように，FULLSET 版と比べ MWS 版で提供する NICTER リソースは，ダークネットトラフィックのみであり，静的・動的ミクロ解析環境を提供する必要が無いためである．さらに，提供されるマクロ解析環境は，Linux のみである．

4 評価

現在，本システムは FULLSET 版，MWS 版共に実験運用を行っている．本章では，運用した際のデータから稼働率を求め可用性に関して示し，運用実績として，登録ユーザ数の推移や，VM 数，全ユーザの日毎のログイン数，VM に対して行った月毎の Import および Export 流量を示す．

4.1 稼働率

以下では，2012 年 1 月から 2014 年 7 月までの実運用における稼働率を示し，可用性に関して評価する．

稼働率の計算は，次式により計算する．

$$\text{稼働率} = \frac{MTBF}{MTBF + MTTR} \qquad (1)$$

期間中，実験運用システムとして稼働していなければならない時間は（法定停電などを除く），22,605 時間（期間中 27 時間停電），期間中に発生した故障による運用停止時間は 42 時間であった．MTBF を 22,605，MTTR を 42 として式 (1) に当てはめ稼働率を計算すると，0.998 となる．

商用サービスのような高可用性（0.9999 以上）とはいかないが，可用性は高いと考えられる．また，著者らが過去に発表したデータでは，2012 年 1 月から 12 月までの稼働率は，0.995 であり [5]，現在の稼働率 0.998 は以前より向上している．

4.2 運用実績

本稿執筆時点での，本システムの解析環境種別毎のユーザ数と VM 数を表 1 に示す．

解析環境	ユーザ数	VM 数
マクロ解析	58 ユーザ	60 台
動的ミクロ解析	14 ユーザ	32 台
静的ミクロ解析	10 ユーザ	10 台
合計	82 ユーザ	102 台

表 1: NONSTOP のユーザ数

表 1 から，現時点では，マクロ解析環境ユーザが多く，本システムは主に，ダークネットトラフィックに関する研究に活用されていることが分かる．

図 3 は，2013 年 4 月 1 日から 2014 年 8 月 2 日までの，日毎のユーザログイン回数と，20 日移動平均を示している．移動平均から，ログイン回数には，大きく 3 つの山が存在し，1 つめ目は，2013 年 6 月から 8 月末まで，2 つ目は，2014 年 11 月から 12 月末まで，3 つ目は，2014 年 4 月中旬からである．これらは，それぞれ，MWS2013，SCIS2014（暗号と情報セキュリティシンポジウム），MWS2014 の原稿・発表資料作成時期と重なる．

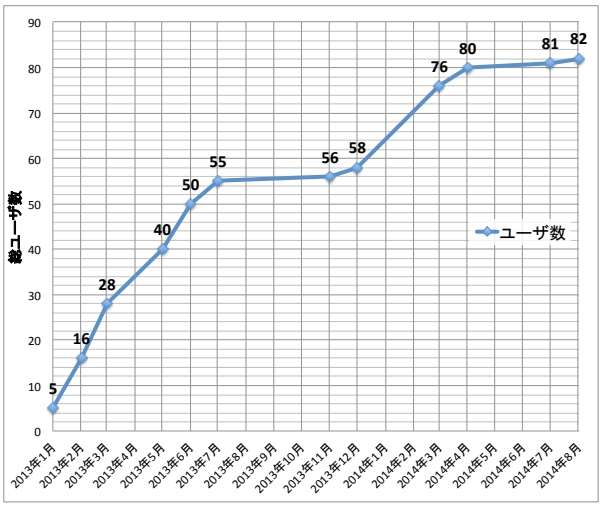

図 4: 登録ユーザ数の推移

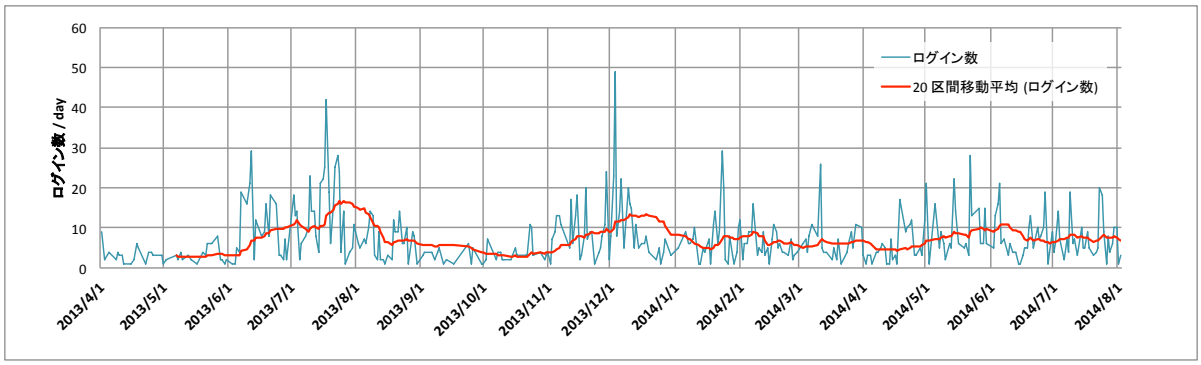

図 3: 日毎のログイン数 (2013/4/1〜2014/8/2)

解析環境	ユーザ数	VM 数
MWS 2013	16 ユーザ	16 台
MWS 2014 (原稿執筆時点)	13 ユーザ	13 台
合計	29 ユーザ	29 台

表 2: NONSTOP MWS のユーザ数

図 4 は，2013 年 1 月から 2014 年 8 月までの本システムへのユーザ登録数である．一般への実験運用開始から，右肩上がりにユーザ数が増えている．また，MWS 版として，表 2 で示すように，MWS2013 では，16 ユーザが利用し，MWS2014 では現時点で 13 ユーザが利用申請している．MWS2013 では，NONSTOP を活用した研究発表が 16 ユーザ中から 6 件あり，また，他の学会においても NONSTOP を利用した研究発表が多数行われている．

図 5 は，2014 年 1 月〜7 月末までの月毎のファイル Import と Export 流量である．また，Import の平均流量は 333MB/月，ピーク時は 1.9GB/月 (5 月) で，Export の平均流量は 671MB/月，ピーク時は 2.5GB/月 (4 月) であった．さらに，2014 年 4 月 24 日は，1 日で 2.3GB/日の Export が発生したが，正常に Export が行われた．この事から，ファイル転送機能の性能としてピーク負荷 2GB/日程度は問題なく処理することができる．

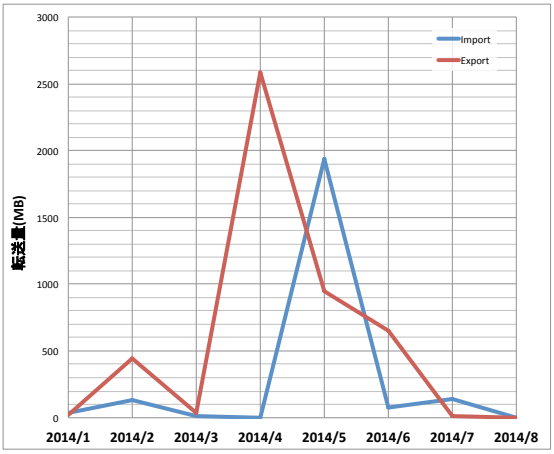

図 5: ファイル入出力量

5 まとめ

本稿では，データセット提供プラットフォームとしての NONSTOP の改良点，追加機能を示し、実稼働させ可用性を評価し，提案システムの有効性を示した．

今後，ますますユーザが増えると予想され，NONSTOP というシステム名が示すように，システムの停止やユーザの研究を停滞させることが無いような，運用体制やシステムの冗長化．性能向上や，VM 上で解析する際のストレスの低減，提供するリソースへのセキュアで簡便なアクセス，解析サンプルソースなどの提供を行うこと，さらに，セキュリティに関する定量的評価が今後の課題である．また，提供するサイバーセキュリティ情報の拡充も順次進めていく予定である．

さらに，本システムは，2013 年度から引き

続き MWS2014 における，NICTER Darknet Dataset2014 の提供の場として利用され，今年度は新たな試みとして，MWS Cup2014 においても利用される．このことからも，本システムは，サイバー攻撃に関する研究者の人材育成，研究の発展に対して大きく貢献できると期待される．

謝辞

NONSTOP の設置・運用に関して多大な協力を頂いた，NICT の高木 彌一郎氏および，システムの開発・運用に関して多大な協力を頂いた，株式会社ニッシンの畑 太一氏に謝意を表する．

参考文献

[1] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, K. Rikitake, “ nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis, ” The 1st Joint Workshop on Information Security (JWIS06), pp. 363 - 377, 2006.

[2] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, “ A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities, ” The 2nd Joint Workshop on Information Security (JWIS07), pp. 267 - 279, 2007.

[3] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, K. Nakao, “ nicter: An Incident Analysis System toward Binding Network Monitoring with Malware Analysis, ” WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 58 - 66, 2008.

[4] nicterWeb, `http://www.nicter.jp/`

[5] 竹久 達也, 井上 大介, 衛藤 将史, 吉岡 克成, 笠間 貴弘, 中里 純二, 中尾 康二, ”サイバーセキュリティ情報遠隔分析基盤 NONSTOP ,” 信学技報, 113(95), 85-90, 2013 年 6 月